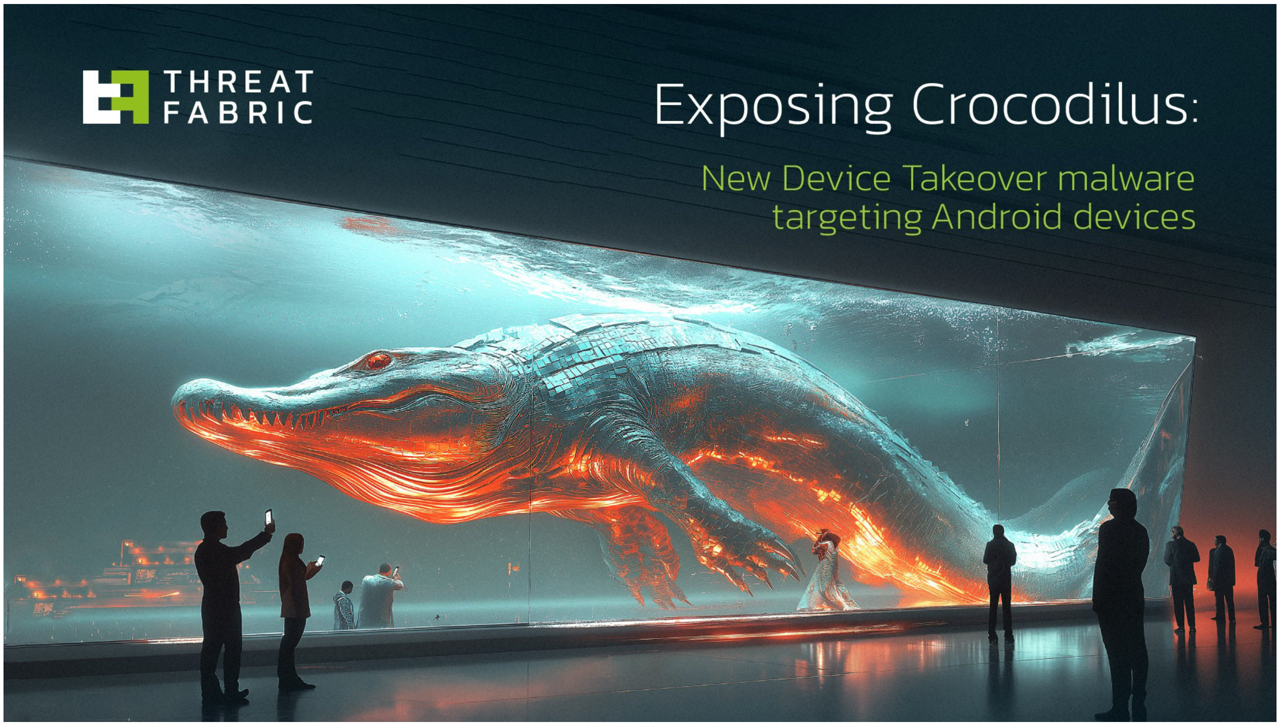
Exposing Crocodilus: New Device Takeover Malware Targeting Android Devices

threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices



Jump to

Introduction

The mobile threat landscape has been shaped over the years by well-established banking Trojan families such as Anatsa, Octo, Hook, each evolving to introduce new techniques for evading detection and maximising financial gain. These malware strains have demonstrated how effective mobile-focused threats can be, particularly when equipped with capabilities like overlay attacks, keylogging, and abuse of Android's Accessibility Services. Their success has not only impacted banks and crypto platforms globally, but also has inspired a growing underground market hungry for similar or improved tools.

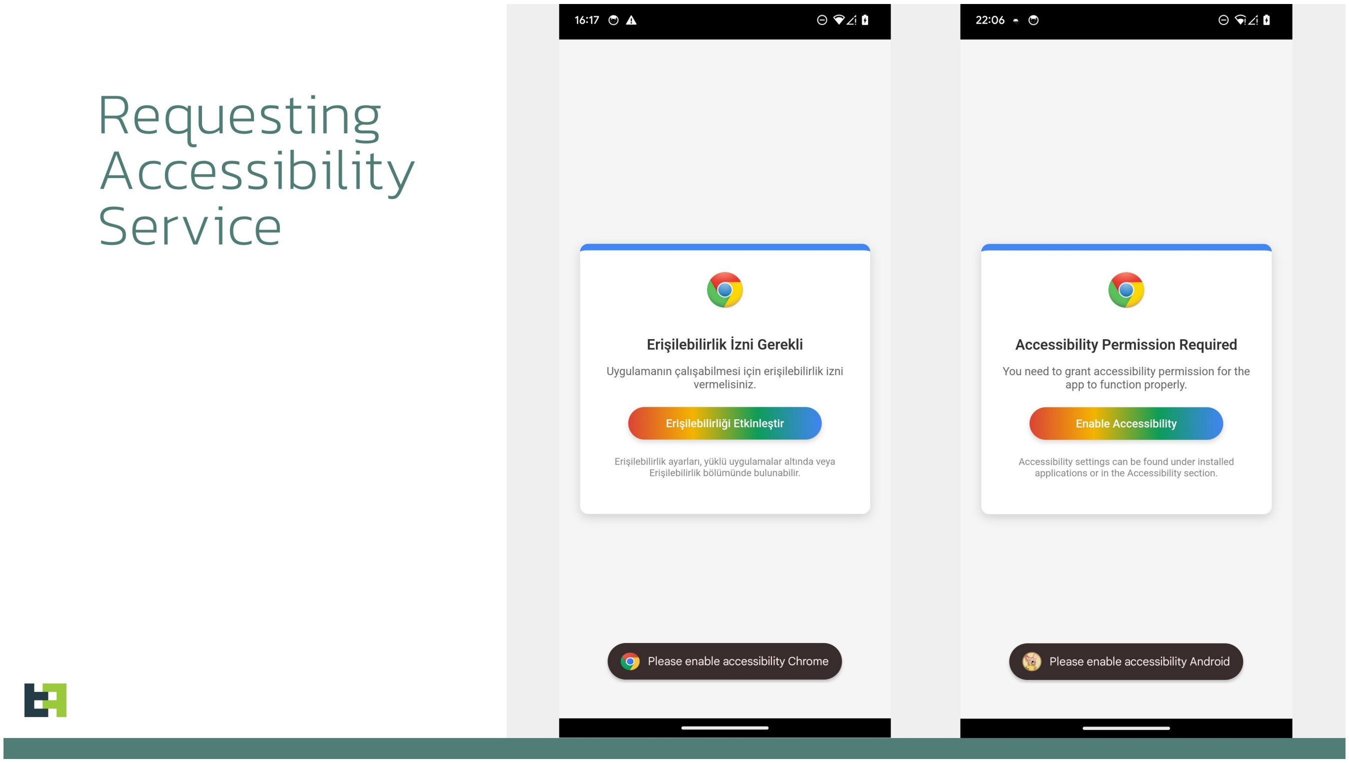
This environment has paved the way for the emergence of **Crocodilus**, a new and highly capable mobile banking Trojan discovered by ThreatFabric.

Crocodilus enters the scene not as a simple clone, but as a fully-fledged threat from the outset, equipped with modern techniques such as remote control, black screen overlays, and advanced data harvesting via accessibility logging. This report explores the features of Crocodilus, its links to known threat actors, and how it lures victims into helping the malware steal their own credentials.

New Name on Threat Landscape

During regular threat hunting operations, our Intel analysts came across previously unseen samples. Analysis revealed a completely new malware family, which we named “Crocodilus” based on references left by the developers (who call it "Crocodile"). Despite being new, it already includes all the necessary features of modern banking malware: overlay attacks, keylogging, remote access, and “hidden” remote control capabilities.

The Modus Operandi of Crocodilus is similar to what we expect from a modern Device Takeover banking Trojan. Initial installation is done via a proprietary dropper [bypassing Android 13+ restrictions](). Once installed, Crocodilus requests Accessibility Service to be enabled.



Requesting Accessibility Service

16:17

Erişilebilirlik İzni Gerekli

Uygulamanın çalışabilmesi için erişilebilirlik izni vermelisiniz.

Erişilebilirliği Etkinleştir

Erişilebilirlik ayarları, yüklü uygulamalar altında veya Erişilebilirlik bölümünde bulunabilir.

Please enable accessibility Chrome

22:06

Accessibility Permission Required

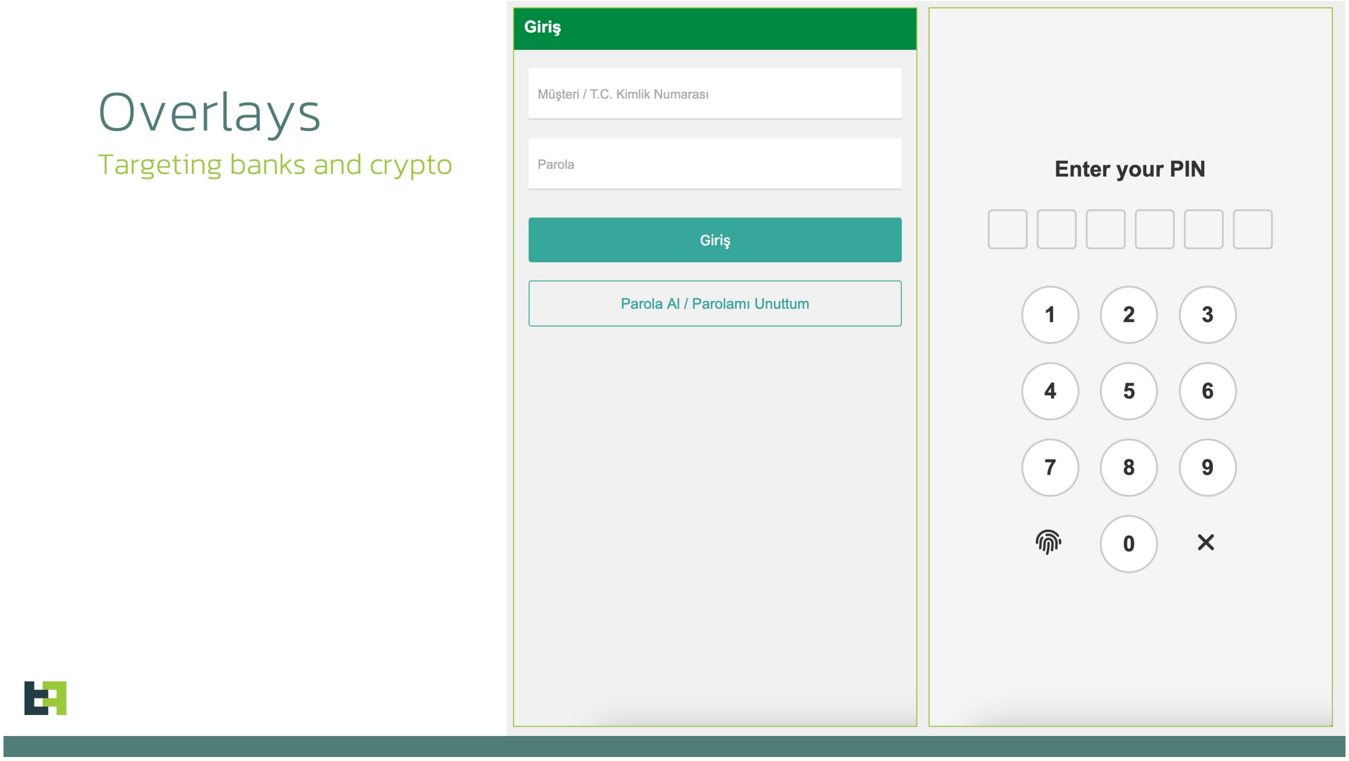
You need to grant accessibility permission for the app to function properly.

Enable Accessibility

Accessibility settings can be found under installed applications or in the Accessibility section.

Please enable accessibility Android

Once granted, the malware connects to the command-and-control (C2) server to receive instructions, including the list of target applications and the overlays to be used. It runs continuously, monitoring app launches and displaying overlays to intercept credentials.



Overlays

Targeting banks and crypto

Initial campaigns observed by our Mobile Threat Intelligence team show targets primarily in Spain and Turkey, along with several cryptocurrency wallets. We expect this scope to broaden globally as the malware evolves.

Another data theft feature of Crocodilus is a keylogger. However, it is more accurate to call it an Accessibility Logger – the malware monitors all Accessibility events and captures all the elements displayed on the screen. In this way, it effectively logs all text changes performed by a victim, making it a keylogger, but the capabilities go beyond just keylogging.

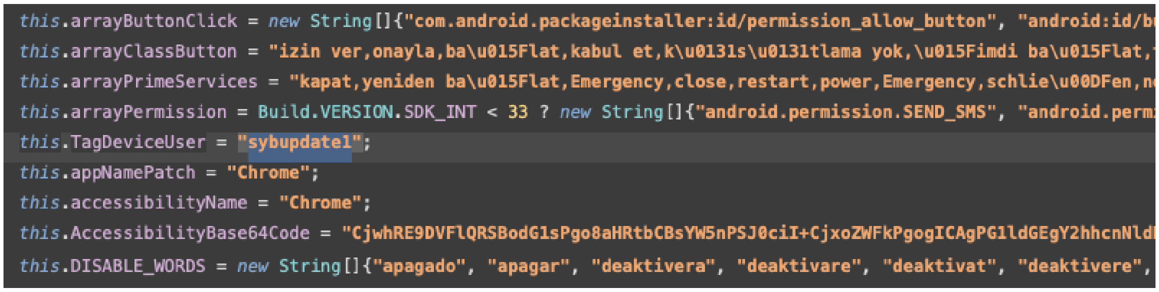
RAT command “*TG32XAZADG*” triggers a screen capture on the content of the Google Authenticator application, and this too is done using the aforementioned Accessibility Logging capabilities. Crocodilus will enumerate all the elements displayed on the screen in Google Authenticator app, capture the text displayed (the name of the OTP code, as well as its value) and send these to the C2, allowing timely theft of OTP codes for the operators of Crocodilus. Bot and RAT commands are listed in the Appendix.

With stolen PII and credentials, threat actors can take full control of a victim’s device using built-in remote access, completing fraudulent transactions without detection.

Crocodilus is also able to make any remote access “hidden” – displaying a black screen overlay on top of all the activities, effectively hiding the actions performed by the malware. As a part of this “hidden” activity the malware also mutes the sound on the infected device to ensure fraudulent activities remain unnoticed by victim.

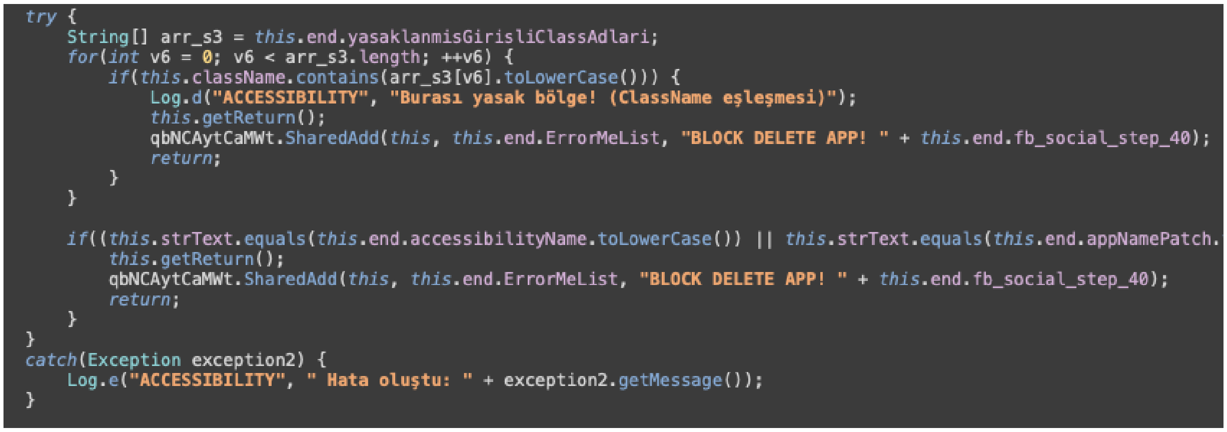
Old Name Behind the Threat

The first Crocodilus samples discovered contain the tag “sybupdate”, which could be linked to a known threat actor in mobile threat landscape, “sybra”, that we already observed operating one of the Ermac forks, "MetaDroid", as well as using Hook and Octo mobile malware. However, it is hard to link "sybra" with the developer of Crocodilus as they might also be a "customer", testing a potential new product entering the market of mobile banking Trojans.



```
this.arrayButtonClick = new String[]{"com.android.packageinstaller:id/permission_allow_button", "android:id/b
this.arrayClassButton = "izin ver,onayla,ba\u015Flat,kabul et,k\u0131s\u0131tlama yok,\u015Fimdi ba\u015Flat,
this.arrayPrimeServices = "kapat,yeniden ba\u015Flat,Emergency,close,restart,power,Emergency,schlie\u00DFen,n
this.arrayPermission = Build.VERSION.SDK_INT < 33 ? new String[]{"android.permission.SEND_SMS", "android.perm
this.TagDeviceUser = "sybupdate1";
this.appNamePatch = "Chrome";
this.accessibilityName = "Chrome";
this.AccessibilityBase64Code = "CjwhRE9DVFlQRSBodG1sPgo8aHRtbCBsYW5nPSJ0ciI+CjxoZWFkPgogICAgPG1ldGEgY2hhcnNld
this.DISABLE_WORDS = new String[]{"apagado", "apagar", "deaktivera", "deaktivare", "deaktivat", "deaktivere",
```

The analysis of the malware source code also reveals debug messages left by the developer(s), based on which we conclude that they are Turkish speaking.

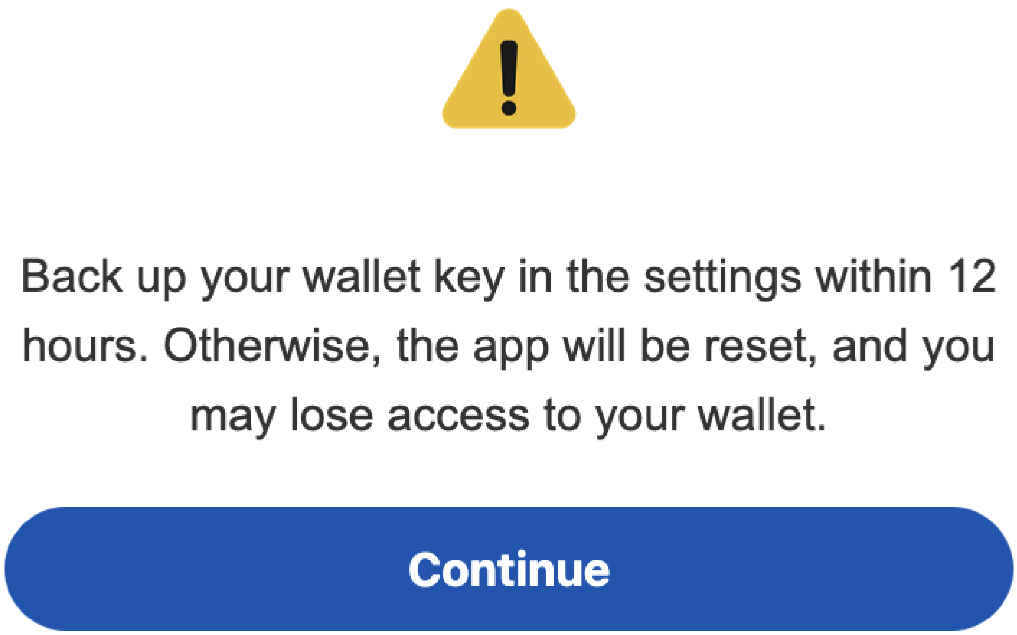


```
try {
    String[] arr_s3 = this.end.yasaklanmisGirisliClassAdlari;
    for(int v6 = 0; v6 < arr_s3.length; ++v6) {
        if(this.className.contains(arr_s3[v6].toLowerCase())) {
            Log.d("ACCESSIBILITY", "Burası yasak bölge! (ClassName eşleşmesi)");
            this.getReturn();
            qbNCAytCaMWt.SharedAdd(this, this.end.ErrorMeList, "BLOCK DELETE APP! " + this.end.fb_social_step_40);
            return;
        }
    }

    if((this.strText.equals(this.end.accessibilityName.toLowerCase()) || this.strText.equals(this.end.appNamePatch.
        this.getReturn();
        qbNCAytCaMWt.SharedAdd(this, this.end.ErrorMeList, "BLOCK DELETE APP! " + this.end.fb_social_step_40);
        return;
    }
}
catch(Exception exception2) {
    Log.e("ACCESSIBILITY", " Hata oluştu: " + exception2.getMessage());
}
```

Making Victims Do the Work

There is one notable detail about overlays targeting cryptocurrency wallets: once a victim provides a password/PIN from the application, the overlay will display a message “*Back up your wallet key in the settings within 12 hours. Otherwise, the app will be reset, and you may lose access to your wallet.*”:



Back up your wallet key in the settings within 12 hours. Otherwise, the app will be reset, and you may lose access to your wallet.

This social engineering trick guides the victim to navigate to their seed phrase (wallet key), allowing Crocodilus to harvest the text using its Accessibility Logger. With this information, attackers can seize full control of the wallet and drain it completely.

Conclusions

The emergence of the Crocodilus mobile banking Trojan marks a significant escalation in the sophistication and threat level posed by modern malware. With its advanced Device-Takeover capabilities, remote control features, and the deployment of black overlay attacks from its earliest iterations, Crocodilus demonstrates a level of maturity uncommon in newly discovered threats.

Already observed targeting banks in Spain and Turkey and popular cryptocurrency wallets, Crocodilus is clearly engineered to go after high-value assets.

The rise of new threats like Crocodilus shows that basic, signature-based detection methods are no longer enough—especially in the early stages when the malware first starts spreading. To stay protected, financial institutions should adopt a layered security approach that includes thorough device and behaviour-based risk analysis on their customers' devices.

Appendix

Bot commands

Command	Description
TR039OQ1QXZXS	Enable call forwarding
DearTetherDest	Perform USSD request
MNKL9G0G9S1XZ	Launch specified application
GoodNightBro	Self-remove from the device
TEB9F0S29KWQ	Post a push notification
RT90SQ28X1Q	Check for available overlays for installed applications
KingOnlyDear	Send SMS to specified number
KingAllDear	Send SMS to all contacts
KingGetDears	Get contact list
KingGetTs	Get installed applications list
KingBoxSex	Get SMS messages
allAdmGet	Request Device Admin privileges
TBL03TSMLS	Bulk send of SMS to specified numbers
TR9S0XZ	Enable black overlay
||SettingsNew||	Update bot settings
||UpdateTr0x910||	Update C2 settings
||FreeApps||	No command, triggers check for created tasks to handle (including overlays download)
chzModes	Enable/disable sound

mkLoper	Lock screen
CsxStx	Enable/disable remote control session
NwSrx	Enable/disable keylogging
mrSemploks	Enable/disable self-protection against deletion
onlineData	List of enabled overlay targets
innaHotLive	Enable/disable update of the target list
SpinderSpike	Make itself a default SMS manager

RAT commands

Command	Description
InfinityGetTo	Start front camera image streaming
InfinityGetStop	Stop front camera image streaming
154856895422	Wake up device screen
TR2XAQSWDEFRGT	Enable/disable “hidden” RAT
RightSlider	Right swipe
LeftSlider	Left swipe
Back_Action	Perform “Back” action
Home_Action	Perform “Home” action
Menu_Action	Perform “Menu” action
864512532655	Down swipe
852147414735	Up swipe
15485666L2	Lock device
M55TRM321XA	Mute phone and enable black overlay
PCROC9F9PCROC	Enable sound and remove overlay
BL03902910AA	Mute phone and enable black overlay
BLD10192OQXX	Enable sound and remove overlay

clickScreen	Perform click
trXSB123QEBASDF	Perform complex gesture
O6155FI2SXZ	Modify text in focused area
TCL9CLSKDLX12	Click a button
messagesLenght	Write in focused area
TG32XAZADG	Capture screen content for Google Authenticator app

IoCs

App name	Package name	SHA256 Hash	C2
Chrome	quizzical.washbowl.calamity	c5e3edafdfda1ca0f0554802bbe32a8b09e8cc48161ed275b8fec6d74208171f	register-buzzy[.]store